(57) 摘要

本发明涉及媒体网关鉴权的方法，包括以下步骤：为媒体网关和媒体网关控制器之间设定一个用于验证双方初始数字签名的初始密钥；所述媒体网关和所述媒体网关控制器用所述初始密钥进行信令通信，以生成新的具有特定生存期的共享密钥；所述媒体网关和所述媒体网关控制器用所述新的共享密钥对呼叫和应答进行鉴权；若所述新的共享密钥的生存期结束，则所述媒体网关和所述媒体网关控制器更新所述共享密钥。本发明能对每个呼叫都进行鉴权，定期更换共享密钥，有效防止不合法呼叫。

媒体网关鉴权的方法

技术领域

本发明涉及通信技术领域，尤其涉及用 MEGACO/MGCP 协议实现媒体网关鉴权方法。

背景技术

媒体网关控制(Media Gateway Control，MEGACO) 协议是因特网工程业务组 (The Internet Engineering Task Force，简称 IETF)的 RFC3015 协议。

如图 1 所示为实现MEGACO 协议的系统组网图。MEGACO 协议采用了分离网关思想，将原来信令和媒体集中处理的网关分解为两部分：媒体网关 (Media Gateway，简称 MG)和媒体网关控制器 (Media Gateway Controller，简称 MGC)。MGC 通过 MEGACO 协议控制 MG 的动作：MGC 向 MG 发出要执行的命令，MG 执行并将结果返回，媒体网关控制器 MGC 也要处理媒体网关 MG 主动上报所发生的事件请求。MEGACO 协议中的逻辑关系是通过连接模型来表示，连接模型中两个最基本的构件就是关联和终结点，关联表示了终结点之间的连接和拓扑关系。

媒体网关控制器 MGC 和媒体网关 MG 之间的主要命令包括 SERVICECHANGE(注册)，ADD(增加)， MODIFY(修改)，SUBTRACT(删除)，NOTIFY(通知)等等。

传统的媒体网关鉴权方法，当媒体网关 MG 注册完成后，通过一个不变的密钥定期对媒体网关 MG 进行鉴权：一方面用同一密钥长时间进行鉴权，易于被第三者破解；另一方面定期鉴权的方法，第三者易于通过只把鉴权消息过滤给真正 MG，使媒体网关控制器 MGC 和媒体网关 MG 之间成功鉴权，而伪造其它的 MG 消息发起呼叫；第三，原有的方法中只有媒体

网关控制器 MGC 对媒体网关 MG 鉴权，因此媒体网关 MG 有可能被不合法的媒体网关控制器 MGC 伪造消息对其呼叫。

发明内容

本发明的目的在于提供一种更加完备的对媒体网关鉴权机制，解决传统 MG 鉴权方法中第三者易于伪造媒体网关 MG 发起呼叫、易于伪造媒体网关控制器 MGC 呼叫媒体网关 MG 以及密钥长时间不变可能被人破解的问题，能对每个呼叫都进行鉴权，能定期更换共享密钥，有效防止不合法的伪造消息对其呼叫。

本发明是这样实现的：

本发明公开了一种媒体网关鉴权的方法，包括：为媒体网关和媒体网关控制器之间设定一个用于验证双方初始数字签名的初始密钥；所述媒体网关和所述媒体网关控制器用所述初始密钥进行信令通信，以生成新的具有特定生存期的共享密钥；所述媒体网关和所述媒体网关控制器用所述新的共享密钥对呼叫和应答进行鉴权；若所述新的共享密钥的生存期结束，则所述媒体网关和所述媒体网关控制器更新所述共享密钥。

优选地，所述生成共享密钥的步骤进一步包括：所述媒体网关向所述媒体网关控制器发起注册信令进行注册，所述注册信令中带有用于生成共享密钥的参数及由所述初始密钥生成的数字签名；所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后，生成共享密钥并设定所述共享密钥的生存期；所述媒体网关控制器对所述媒体网关发起修改命令，所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共享密钥的生存期；所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后，生成共享密钥并设定所述共享密钥的生存期。

优选地，所述鉴权步骤进一步包括：所述媒体网关控制器用所述共享密钥在每次对媒体网关的呼叫消息中进行数字签名；所述媒体网关用所述共享密钥对所述呼叫消息中的所述数字签名进行验证，若合法，则

返回给所述媒体网关控制器带有用所述共享密钥数字签名的应答消息；所述媒体网关控制器用所述共享密钥对所述应答消息中的所述数字签名进行验证，若合法，则建立呼叫，否则，拒绝此次呼叫。

优选地，所述更新共享密钥的步骤进一步包括：所述媒体网关向所述媒体网关控制器发送通知命令，请求所述媒体网关控制器生成新的共享密钥，所述通知命令中带有用于生成共享密钥的参数和由所述初始密钥生成的数字签名；所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后，生成新的共享密钥并设定所述共享密钥的生存期；所述媒体网关控制器对所述媒体网关发起修改命令，所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共享密钥的生存期；所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后，生成共享密钥并设定所述共享密钥的生存期。

优选地，所述媒体网关控制器和所述媒体网关生成共享密钥采用的算法与所述媒体网关控制器和所述媒体网关生成数字签名的算法为不同的算法。

优选地，所述生成共享密钥的参数和数字签名的传送可以通过扩展协议的字段或包来实现。

优选地，所述共享密钥的生存期可以是时间，也可以是新的共享密钥可用于鉴权的次数。

采用本发明技术方案的有益效果，不仅能够定期更换密钥，防止长时间用同一密钥鉴权易于被破解；能够对媒体网关 MG 发起的每一个呼叫进行鉴权，解决了第三者通过过滤消息发起非法呼叫的问题；还能够防止媒体网关 MG 被不合法的媒体网关控制器 MGC 控制完成呼叫。

附图说明

图 1 示出了 MEGACO 协议系统的原理图；

图 2 示出了本发明实现媒体关网关鉴权的流程示意图。

具体实施方式

本发明公开了一种媒体网关鉴权的方法，包括以下步骤：

设定媒体网关 MG 和媒体网关控制器 MGC 之间生成共享密钥采用的算法为 $y=f_1(x)$，设定 MG 和 MGC 之间生成数字签名采用的算法为 $y=f_2(x)$；所述媒体网关控制器和所述媒体网关生成共享密钥的算法，以及所述媒体网关控制器和所述媒体网关生成数字签名的算法，可以根据安全级别的需要而采用合适算法，本发明对具体所用的算法不做限定。

媒体网关 MG 和媒体网关控制器 MGC 之间初始配有一个用于验证双方初始数字签名的密钥 S，媒体网关 MG 和媒体网关控制器 MGC 的密钥 S 可以不同，只要能验证对方的数字签名即可；密钥及参数的传送可以通过扩展 MEGACO 字段或包来实现。

媒体网关 MG 首先向媒体网关控制器 MGC 发起注册信令注册，并带有生成共享密钥的参数及数字签名。媒体网关控制器 MGC 验证合法后生成共享密钥，用修改命令发送给媒体网关 MG 生成共享密钥的参数、数字签名及设定共享密钥生存期，媒体网关 MG 收到后验证数字签名合法将生成共享密钥。

在后续的媒体网关控制器 MGC 和媒体网关 MG 之间的每一个呼叫建立及应答的消息中，媒体网关控制器 MGC 和媒体网关 MG 用共享密钥进行签名，相互验证合法后进行呼叫，否则拒绝呼叫。

当共享密钥生存期结束以后，媒体网关控制器 MGC 使原有的密钥无效；媒体网关 MG 需立刻用通知命令请求媒体网关控制器 MGC 生成新的共享密钥及获取新密钥的生存期。

如此不断变化密钥并用新的密钥对呼叫鉴权。

下面将结合附图，举例说明本发明的一个实施的方式。

图 2 所示的一种实现 MG 鉴权的详细过程。设定 MG 和 MGC 之间的初始密钥为 S。

201) 媒体网关 MG 向媒体网关控制器 MGC 发起注册消息，消息中带有用于媒体网关控制器 MGC 生成共享密钥的信息 M，并带有用密钥 S 对共

享密钥的信息 M 或注册消息生成的数字签名；

202）媒体网关控制器 MGC 收到该消息后用密钥 S 验证数字签名，如果成功则用共享密钥的信息 M 生成共享密钥 S′，并给媒体网关 MG 应答成功；

203）媒体网关控制器 MGC 给媒体网关 MG 发修改（MODIFY）消息，消息中带有用于媒体网关 MG 生成共享密钥的信息 N，并带有用密钥 S 对共享密钥的信息 N 或整个消息生成的数字签名，同时还带有新的共享密钥生存期：生存期可以是一个时间，也可以是新的共享密钥可用于鉴权的次数；

204）媒体网关 MG 收到该消息后用密钥 S 验证数字签名，如果成功则用共享密钥的信息 N 生成共享密钥 S′，并给媒体网关控制器 MGC 应答成功；

205）在以后的每次呼叫建立的某个消息（比如 ADD）中，媒体网关控制器 MGC 用新的共享密钥 S′进行数字签名；

206）媒体网关 MG 收到该消息后用新的共享密钥 S′验证数字签名，如果成功证明是合法的媒体网关控制器 MGC；对媒体网关控制器 MGC 的应答也用新的共享密钥 S′进行数字签名，媒体网关控制器 MGC 收到后用新的共享密钥 S′验证成功后建立呼叫，否则为非法的媒体网关 MG，拒绝该呼叫；在媒体网关控制器 MGC 对媒体网关 MG 的定期鉴权中也用同样的方法；

207）当媒体网关控制器 MGC 设定的共享密钥生存期结束后，媒体网关 MG 向媒体网关控制器 MGC 上报通知（NOITFY）消息，消息中带有用于媒体网关控制器 MGC 生成共享密钥的信息 M′，并带有用密钥 S 对共享密钥的信息 M′或整个消息生成的数字签名；

208）媒体网关控制器 MGC 收该消息后用密钥 S 验证数字签名，如果成功则用共享密钥的信息 M′生成共享密钥 S′′，并给媒体网关 MG 应答成功；

209）媒体网关控制器 MGC 给媒体网关 MG 发修改（MODIFY）消息，

消息中带有用于媒体网关 MG 生成共享密钥的信息 N′，并带有用密钥 S 对共享密钥的信息 N′或整个消息生成的数字签名，同时还带有新的共享密钥生存期；媒体网关 MG 用共享密钥的信息 N′生成新的共享密钥 S′′，并用新的共享密钥 S′′对后续呼叫鉴权及定期鉴权；

210)媒体网关 MG 给媒体网关控制器 MGC 成功的应答。

新的共享密钥 S′′′生存期到后再重复 207)—210)步骤生成新的共享密钥 S′′′′，依次类推。

尽管参照实施例对所公开的涉及使用 MEGACO 协议实现对媒体网关鉴权的方法进行了特别描述，本领域技术人员将能理解，在不偏离本发明的范围和精神的情况下，可以对它进行形式和细节的种种显而易见的修改。例如，由于 MEGACO 协议和 MGCP 协议的相似性，本法的技术方案的实质内同对于使用 MGCP 协议实现媒体网关鉴权同样适用。因此，以上描述的实施例是说明性的而不是限制性的，在不脱离本发明的精神和范围的情况下，所有的变化和修改都在本发明的范围之内。

权利要求

1. 一种媒体网关鉴权的方法，其特征在于，该方法包括：

为媒体网关和媒体网关控制器之间设定一个用于验证双方初始数字签名的初始密钥；

所述媒体网关和所述媒体网关控制器用所述初始密钥进行信令通信，以生成新的具有特定生存期的共享密钥；

所述媒体网关和所述媒体网关控制器用所述新的共享密钥对呼叫和应答进行鉴权；

若所述新的共享密钥的生存期结束，则所述媒体网关和所述媒体网关控制器更新所述共享密钥。

2. 如权利要求 1 所述的方法，其特征在于，所述生成共享密钥的步骤进一步包括：

所述媒体网关向所述媒体网关控制器发起注册信令进行注册，所述注册信令中带有用于生成共享密钥的参数及由所述初始密钥生成的数字签名；

所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后，生成共享密钥并设定所述共享密钥的生存期；

所述媒体网关控制器对所述媒体网关发起修改命令，所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共享密钥的生存期；

所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后，生成共享密钥并设定所述共享密钥的生存期。

3. 如权利要求 1 所述的方法，其特征在于，所述鉴权步骤进一步包括：

所述媒体网关控制器用所述共享密钥在每次对媒体网关的呼叫消息中进行数字签名；

所述媒体网关用所述共享密钥对所述呼叫消息中的所述数字签名进行验证，若合法，则返回给所述媒体网关控制器带有用所述共享密钥数

字签名的应答消息;

所述媒体网关控制器用所述共享密钥对所述应答消息中的所述数字签名进行验证，若合法，则建立呼叫，否则，拒绝此次呼叫。

4. 如权利要求 1 所述的方法，其特征在于，所述更新共享密钥的步骤进一步包括:

所述媒体网关向所述媒体网关控制器发送通知命令，请求所述媒体网关控制器生成新的共享密钥，所述通知命令中带有用于生成共享密钥的参数和由所述初始密钥生成的数字签名;

所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后，生成新的共享密钥并设定所述共享密钥的生存期;

所述媒体网关控制器对所述媒体网关发起修改命令，所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共享密钥的生存期;

所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后，生成共享密钥并设定所述共享密钥的生存期。

5. 如权利要求 2、3 或 4 所述的方法，其特征在于，所述媒体网关控制器和所述媒体网关生成共享密钥采用的算法与所述媒体网关控制器和所述媒体网关生成数字签名的算法为不同的算法。

6. 如权利要求 2、3 或 4 所述的方法，其特征在于，所述生成共享密钥的参数和数字签名的传送可以通过扩展协议的字段或包来实现。

7. 如权利要求 1 所述的方法，其特征在于，所述共享密钥的生存期可以是时间，也可以是新的共享密钥可用于鉴权的次数。

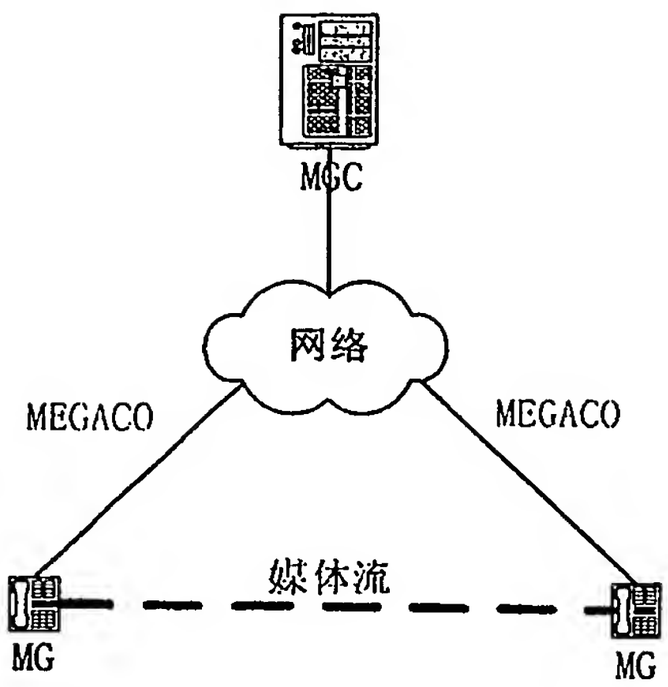
MGC
网络
MEGACO
MEGACO
媒体流
MG
MG

图 1

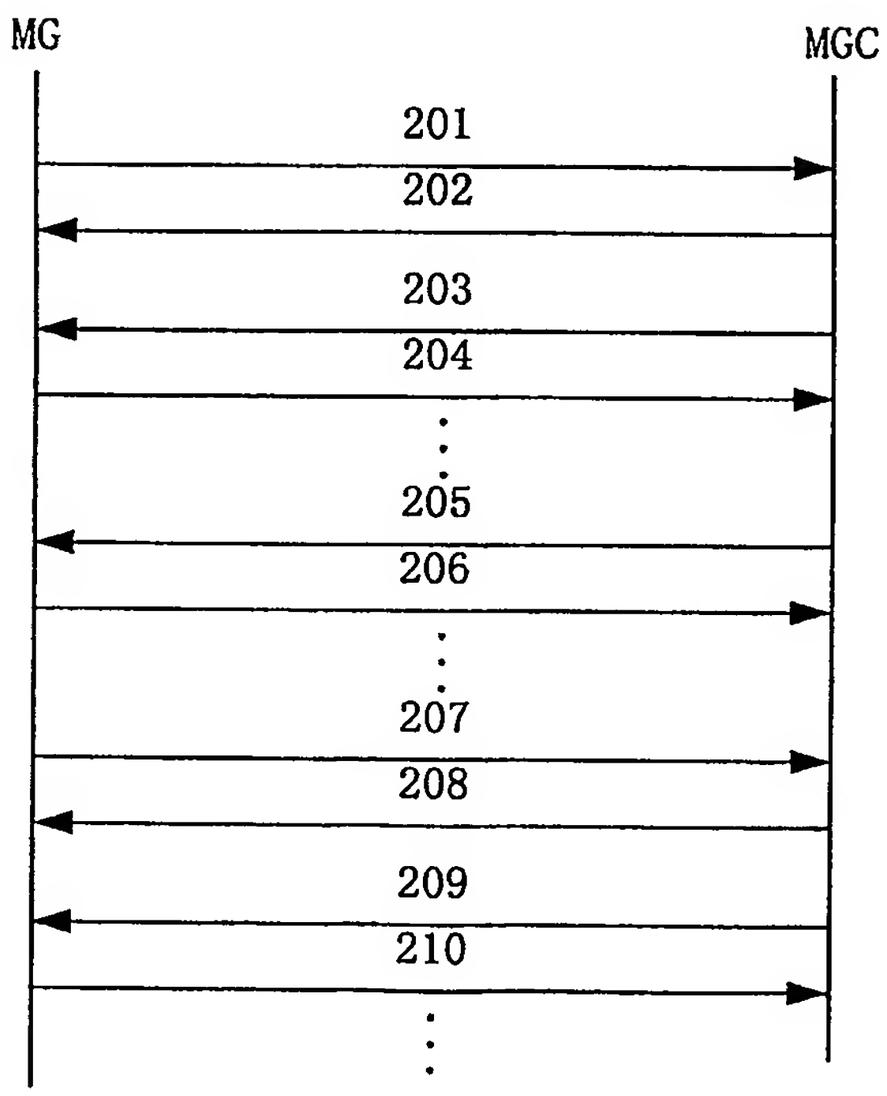
MG
MGC
201
202
203
204
205
206
207
208
209
210

图 2